EXHIBIT A

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 17-sw-5751-KLM
Affordable Inns – Denver West, Room 149, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033, more fully described in Attachment A, attached hereto.	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed *(identify the person or describe the property to be seized):*

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Fraud and related activity in connection with computers

The application is based on these facts:

X Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Brian W. Behm
Applicant's signature

[Insert Agents name, Title and Agency name]
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***26 May 2017***

Judge's signature

City and state: Denver, CO

Kristen L. Mix
United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brian W. Behm, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since May 2004. I am currently assigned to the Minneapolis Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, Internet and computer intrusion offenses.

2. During my career as a Special Agent of the FBI, I have participated in numerous investigations involving computer-related offenses, and assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information. In addition to graduating from the FBI Academy in Quantico, Virginia, I have received both formal and informal training in computer-related investigations from the FBI and other organizations.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search the place named in Attachment A.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates, 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly

cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."

6. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 1030(a)(5)(A), which relate to the execution of a DDoS attack (the "Subject Offense").

7. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, are presently located at the place described in Attachment A.

8. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Background

9. The Internet is a worldwide network of computers, computer systems, and other devices. Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

10. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally

associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

11. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

PROBABLE CAUSE

12. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting its website, www.washburngrp.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shut-down of its website. The attacks have continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

13. I have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

14. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee of Washburn. The email addresses both contained the name, of an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago: "LXXXX SXXXXXXXXXX."[1] The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

15. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

16. Subscriber information was obtained from Google on the account lXXXXsXXXXXXXXXX15@gmail.com, and from Yahoo for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Centurylink's records reflect this IP address was assigned to Gammell's address (4975 Mother Lode Trail, Las Cruces, New Mexico 88011)

[1] Where email addresses or other personally identifiable information of non-targets of this investigation are referenced herein, your affiant has redacted portions of the identifying information to protect the identity of those third parties using "XXX..." In each instance, your affiant knows the full, unredacted identifier.

at the time the account was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

17. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

18. I discovered that Gammell maintains numerous social media accounts, to include Facebook, Twitter, LinkedIn, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed by business records obtained from Google.

Search Warrant Results – jkgammell@gmail.com

19. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. I reviewed the records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

20. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

21. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled

"vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

22. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, I located payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

23. The website cstress.net is not currently active, however I have reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

24. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of $28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two October 20, 2015

emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

25. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

26. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

27. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

28. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

29. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

30. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and

> powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

31. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

32. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

vDOS Records

33. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016. I have verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information I obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that I obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, I was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS

records with receipts for those payments that I located in Gammell's Gmail account I obtained via search warrant.

34. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's jkgammell@gmail.com email address.

35. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

36. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

37. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

38. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Business records from Centurylink show IP address 75.161.68.161

was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from lXXXXsXXXXXXXXXX15@gmail.com. As mentioned above, email account lXXXXsXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

39. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. I was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

1. Wells Fargo (two IP addresses);

2. JP Morgan Chase Bank;

3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on my review of the

jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on my review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on my review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

40. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

41. On February 3, 2017, FBI agents conducting surveillance of 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 observed a white Buick Century bearing New Mexico license plate NYY328 parked in the driveway. On February 9, 2017, an FBI agent in New Mexico queried New Mexico's Online Motor Vehicle Record System and learned that Gammell is the registered owner of a white 2003 Buick Century, New Mexico license plate NYY328 (the "SUBJECT VEHICLE"). The vehicle was registered on November 30, 2016, listing Gammell's previous address as 4975 Mother Lode Trail, Las Cruces, New Mexico 88011.

42. On May 1, 2017, FBI agents in Colorado observed Gammell's known vehicle, a 2003 white Buick Century bearing New Mexico license plate NYY328, parked in the Affordable Inns – Denver West, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033 parking lot. Shortly after locating the vehicle, agents saw Gammell entering the vehicle and departing the Affordable Inns – Denver West parking lot. Based on my investigation, your affiant knows that Gammell works short-term jobs around the country. Since approximately April 2015, Gamell has lived with his parents in Las Cruces, New Mexico, but periodically travels for work. Based on your affiant's knowledge of Gammell's work history, he appears to be currently in Denver, Colorado for that purpose.

43. On May 1, 2017, an FBI Task Force member in Colorado contacted the Affordable Inns – Denver West staff and requested a rental roll. A review of the rental roll showed Gammell was staying in Room 149.

44. On May 5, 2017, the United States District Court for the District of Minnesota issued a Pen Register and Trap and Trace order for Gammell's email account, jkgammell@gmail.com. A review of the data generated by the order found IP address 76.120.18.178 frequently was used to login to jkgammell@gmail.com on May 9, 2017 and May 10, 2017, with the logins occurring between approximately 9:00pm and 6:30am Mountain Standard Time. Law enforcement requested subscriber information on IP address 76.120.18.178 on May 9, 2017 and May 10, 2017 from Comcast. On May 24,

2017, Comcast reported that on May 9, 2017 and May 10, 2017, IP address 76.120.18.178 was assigned to Affordable Inns, 10300 South I70 Frontage Road, Wheat Ridge, Colorado 80033. Gammell's use of the hotel internet connection shows he has computer equipment in his possession. In my training and experience, people keep their computers both in their residences, and they keep or transport their computers using their cars. Gammell's computer equipment may have been used in furtherance of his DDoS activity described below, and consequently may contain evidence of the DDoS activity.

Computers and Telephones

45. Your affiant requests permission to search for and seize the records, documents, and/or materials described in the Attachment B ("Items To Be Seized"). These records, documents, and materials may constitute evidence and/or instrumentalities of crime. These items may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

46. These records, documents, and/or materials may be in the form of paper or stored in the form of computer hardware, software, and electronic files. Businesses and individuals use computers and cell phones at their business and residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.

47. This affidavit also requests permission to seize computer hardware and cell phones that may contain records and documents if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In fact, both Google (which operates Gmail) and Twitter offer dedicated apps for their customers' cell phones.

48. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for

forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls

for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive (or similar media) to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

51. Based on the facts and background information set forth above, I respectfully submit there is probable cause to believe that evidence of a criminal offense, namely, violation of 18 U.S.C. § 1030, is

located within the place described in Attachment A, which is more fully described in Attachment A, attached hereto and incorporated herein.

52. I, therefore, respectfully request that a search warrant be issued authorizing the search of the residence described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein by reference.

s/ Brian W. Behm
Brian W. Behm
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me this 26th day of May 2017

United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Judith Smith, Assistant United States Attorney.

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as hotel room number 149 at the Affordable Inns – Denver West, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033. The hotel is at the intersection of Interstate 70 Frontage Road South and Miller Street, on the east side of Miller Street.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related to the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

1. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;
2. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;
3. Records related to the email addresses jkgammell@gmail.com, and thepicklator@aol.com;
4. Records related to the email addresses ending in @yahoo.com or 15@gmail.com that also contain the name of former Washburn Computer Group employees.
5. Records related to payments made to DDoS-for-hire services;
6. Records related to the use of Coinbase;
7. Records related to the moniker "anonrooster,"
8. Records related to the moniker "AnonCunnilingus";
9. Records related to the online group "Anonymous";
10. Records reflecting conduct in violation of 18 U.S.C. § 1030;

11. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media

EXHIBIT B

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A white 2003 Buick Century bearing New Mexico license plate NYY328	Case No. 17-sw-5750-KLM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed *(identify the person or describe the property to be seized):*

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Fraud and related activity in connection with computers

The application is based on these facts:

X Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature
s/Brian W. Behm
[Insert Agents name, Title and Agency name]
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***26 May 2017***

Judge's signature
Kristen L. Mix
United States Magistrate Judge
Printed name and title

City and state: Denver, CO

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brian W. Behm, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since May 2004. I am currently assigned to the Minneapolis Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, Internet and computer intrusion offenses.

2. During my career as a Special Agent of the FBI, I have participated in numerous investigations involving computer-related offenses, and assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information. In addition to graduating from the FBI Academy in Quantico, Virginia, I have received both formal and informal training in computer-related investigations from the FBI and other organizations.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search the place named in Attachment A.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates, 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly

cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."

6. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 1030(a)(5)(A), which relate to the execution of a DDoS attack (the "Subject Offense").

7. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, are presently located at the place described in Attachment A.

8. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Background

9. The Internet is a worldwide network of computers, computer systems, and other devices. Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

10. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally

associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

11. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

PROBABLE CAUSE

12. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting its website, www.washburngrp.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shut-down of its website. The attacks have continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

13. I have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

14. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee of Washburn. The email addresses both contained the name, of an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago: "LXXXX SXXXXXXXXXX."[1] The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

15. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

16. Subscriber information was obtained from Google on the account lXXXXsXXXXXXXXXX15@gmail.com, and from Yahoo for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Centurylink's records reflect this IP address was assigned to Gammell's address (4975 Mother Lode Trail, Las Cruces, New Mexico 88011)

[1] Where email addresses or other personally identifiable information of non-targets of this investigation are referenced herein, your affiant has redacted portions of the identifying information to protect the identity of those third parties using "XXX..." In each instance, your affiant knows the full, unredacted identifier.

at the time the account was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

17. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

18. I discovered that Gammell maintains numerous social media accounts, to include Facebook, Twitter, LinkedIn, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed by business records obtained from Google.

Search Warrant Results – jkgammell@gmail.com

19. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. I reviewed the records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

20. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

21. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled

"vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

22. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, I located payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

23. The website cstress.net is not currently active, however I have reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

24. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of $28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two October 20, 2015

emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

25. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

26. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

27. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

28. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

29. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

30. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and

> powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

31. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

32. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

vDOS Records

33. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016. I have verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information I obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that I obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, I was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS

records with receipts for those payments that I located in Gammell's Gmail account I obtained via search warrant.

34. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's jkgammell@gmail.com email address.

35. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

36. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

37. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

38. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Business records from Centurylink show IP address 75.161.68.161

was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from lXXXXsXXXXXXXXXX15@gmail.com. As mentioned above, email account lXXXXsXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

39. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. I was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

1. Wells Fargo (two IP addresses);

2. JP Morgan Chase Bank;

3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on my review of the

jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on my review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on my review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

40. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

41. On February 3, 2017, FBI agents conducting surveillance of 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 observed a white Buick Century bearing New Mexico license plate NYY328 parked in the driveway. On February 9, 2017, an FBI agent in New Mexico queried New Mexico's Online Motor Vehicle Record System and learned that Gammell is the registered owner of a white 2003 Buick Century, New Mexico license plate NYY328 (the "SUBJECT VEHICLE"). The vehicle was registered on November 30, 2016, listing Gammell's previous address as 4975 Mother Lode Trail, Las Cruces, New Mexico 88011.

42. On May 1, 2017, FBI agents in Colorado observed Gammell's known vehicle, a 2003 white Buick Century bearing New Mexico license plate NYY328, parked in the Affordable Inns – Denver West, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033 parking lot. Shortly after locating the vehicle, agents saw Gammell entering the vehicle and departing the Affordable Inns – Denver West parking lot. Based on my investigation, your affiant knows that Gammell works short-term jobs around the country. Since approximately April 2015, Gamell has lived with his parents in Las Cruces, New Mexico, but periodically travels for work. Based on your affiant's knowledge of Gammell's work history, he appears to be currently in Denver, Colorado for that purpose.

43. On May 1, 2017, an FBI Task Force member in Colorado contacted the Affordable Inns – Denver West staff and requested a rental roll. A review of the rental roll showed Gammell was staying in Room 149.

44. On May 5, 2017, the United States District Court for the District of Minnesota issued a Pen Register and Trap and Trace order for Gammell's email account, jkgammell@gmail.com. A review of the data generated by the order found IP address 76.120.18.178 frequently was used to login to jkgammell@gmail.com on May 9, 2017 and May 10, 2017, with the logins occurring between approximately 9:00pm and 6:30am Mountain Standard Time. Law enforcement requested subscriber information on IP address 76.120.18.178 on May 9, 2017 and May 10, 2017 from Comcast. On May 24,

2017, Comcast reported that on May 9, 2017 and May 10, 2017, IP address 76.120.18.178 was assigned to Affordable Inns, 10300 South I70 Frontage Road, Wheat Ridge, Colorado 80033. Gammell's use of the hotel internet connection shows he has computer equipment in his possession. In my training and experience, people keep their computers both in their residences, and they keep or transport their computers using their cars. Gammell's computer equipment may have been used in furtherance of his DDoS activity described below, and consequently may contain evidence of the DDoS activity.

Computers and Telephones

45. Your affiant requests permission to search for and seize the records, documents, and/or materials described in the Attachment B ("Items To Be Seized"). These records, documents, and materials may constitute evidence and/or instrumentalities of crime. These items may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

46. These records, documents, and/or materials may be in the form of paper or stored in the form of computer hardware, software, and electronic files. Businesses and individuals use computers and cell phones at their business and residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.

47. This affidavit also requests permission to seize computer hardware and cell phones that may contain records and documents if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In fact, both Google (which operates Gmail) and Twitter offer dedicated apps for their customers' cell phones.

48. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for

forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls

for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive (or similar media) to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

51. Based on the facts and background information set forth above, I respectfully submit there is probable cause to believe that evidence of a criminal offense, namely, violation of 18 U.S.C. § 1030, is

located within the place described in Attachment A, which is more fully described in Attachment A, attached hereto and incorporated herein.

52. I, therefore, respectfully request that a search warrant be issued authorizing the search of the residence described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein by reference.

s/ Brian W. Behm
Brian W. Behm
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me this 26th day of May 2017

United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Judith Smith, Assistant United States Attorney.

ATTACHMENT A

Description of Location to be Searched

The SUBJECT VEHICLE is specifically described white 2003 Buick Century, New Mexico license plate NYY328.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related to the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

1. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;
2. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;
3. Records related to the email addresses jkgammell@gmail.com, and thepicklator@aol.com;
4. Records related to the email addresses ending in @yahoo.com or 15@gmail.com that also contain the name of former Washburn Computer Group employees.
5. Records related to payments made to DDoS-for-hire services;
6. Records related to the use of Coinbase;
7. Records related to the moniker "anonrooster,"
8. Records related to the moniker "AnonCunnilingus";
9. Records related to the online group "Anonymous";
10. Records reflecting conduct in violation of 18 U.S.C. § 1030;

11. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media

EXHIBIT C

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 06/13/2017

JOHN GAMMELL, date of birth (DOB) December 4, 1962, address 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, telephone number 612-205-8609, email address jkgammell@gmail.com, was interviewed at the Denver Field Office of the FEDERAL BUREAU OF INVESTIGATION (FBI), 8000 East 36th Avenue, Denver, Colorado 80238 pursuant to his arrest. GAMMELL was advised of the identities of the interviewing Agents and the purpose of the interview. GAMMELL was then provided with an "Advice of Rights" form, which was read to him and he was allowed to read as well. GAMMELL stated he understood his rights but declined to sign the form, however, GAMMELL indicated he wished to talk with the interviewing Agents. Thereafter, GAMMELL provided the following information:

The below section is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties in the interview room were electronically recorded. The recording captures the actual words spoken. The recording began on May 31, 2017 at approximately 7:08am Mountain Daylight Time (MDT), and the recording concluded on May 31, 2017 at approximately 7:57am MDT.

SUMMARY OF RECORDED INTERVIEW

GAMMELL began working for Washburn Computer Group (WCG) in Minnesota in approximately 2005 or 2006. GAMMELL'S last contact with WCG was regarding the cancellation of training GAMMELL was to provide to WCG. GAMMELL knows Loren Stoltenberg from his time working at WCG. GAMMELL denied ever creating email accounts utilizing Stoltenberg's name.

GAMMELL claimed not to know what a distributed denial of service (DDoS) attack was, and denied any knowledge or involvement in executing DDoS attacks, to include any attacks involving WCG. GAMMELL was not aware of any online companies providing DDoS-for-hire services. GAMMELL did not recognize the names of the DDoS-for-hire services vDOS, cstress.net, or booter.xyz. GAMMELL denied using his Paypal account to make purchases from DDoS-for-hire services. GAMMELL said he is not a computer hacker.

GAMMELL provided his email address as jkgammell@gmail.com, and he has used the account for between eight to ten years.

GAMMELL was aware of the group 'Anonymous', but preferred not to answer any questions about having contact with members of the group 'Anonymous'.

GAMMELL was interested in pursuing a cyber security career. GAMMELL was learning how to use Linux via udemy.com.

GAMMELL does not use encryption software on his computers. GAMMELL was familiar with CCleaner and utilizes it on his computer.

GAMMELL was shown a picture of a keychain with three keys that were found in his hotel room. One of the keys had a white base and the number 173 written in black ink on the white portion of the key. GAMMELL did not remember what the key was for, adding that it was potentially a mailbox key.

GAMMELL intended to build an AR15 with the AR15 components he had stored in his hotel room. GAMMELL had a friend who was going to help him through the process. GAMMELL ordered the weapons online and had yet to assemble the weapon. GAMMELL would not identify the friend who was going to help him assemble the AR15.

GAMMELL had not gone to a shooting range since arriving in Denver. GAMMELL was not familiar with the Family Shooting Center in Aurora, Colorado.

GAMMELL did not have any knowledge about an H and K handgun case found near his belongings at his father's house in New Mexico.

NON RECORDED INTERVIEW

AGENT NOTE: While sitting in an FBI vehicle in the sally port waiting for processing at the US Federal Courthouse, 901 19th Street, Denver, Colorado 80294, GAMMELL began making additional statements to the interviewing Agents. The following information provided by GAMMELL was not recorded.

GAMMELL stated the FBI will not be able to recover any data from the computer seized from GAMMELL'S residence in New Mexico as he wiped the computer at least four times, to Department of Defense standards, prior to temporarily relocating to Denver. GAMMELL then began discussing the external hard drive seized from his hotel room in Wheat Ridge. GAMMELL stated he encrypted the hard drive using three different methods, claiming

FD-302a (Rev. 05-08-10)

288A-MP-6766321

Continuation of FD-302 of (U) Interview of John Gammell , On 05/31/2017 , Page 3 of 3

not even the National Security Agency would be able to access the data on the drive. One of the methods GAMMELL used to encrypt the drive was Veracrypt. GAMMELL stated he "would owe a beer" to the interviewing Agents if the encryption on the drive could be defeated.

GAMMELL'S parents in New Mexico were his adoptive parents. GAMMELL'S biological mother gave him up for adoption at birth. GAMMELL'S biological mother, BETH FUNK, hired a private investigator to locate GAMMELL in approximately 2000. FUNK owns an art studio in the Denver area called Colorado Clay Studio. Colorado Clay Studio is located at 6859 Leetsdale Drive. GAMMELL spent time at his mother's studio while temporarily working in the Denver area. While at FUNK'S studio, GAMMELL utlized a 15" Lenovo laptop and left the laptop at the studio. The studio did not have internet service, so GAMMELL would go to the bar next door and use the wireless internet connection.

EXHIBIT D

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Storage Unit #173 at Discount Storage, located at 2499 Camino Real, Las Cruces, New Mexico 88007

Case No. 17MR491

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Storage Unit #173 at Discount Storage, located at 2499 Camino Real, Las Cruces, New Mexico 88007, more fully described in Attachment A, which is attached and fully incorporated herein.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and fully incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1030(a)(5)(A)	Intentional Damage to a Protected Computer
18 USC 922(g)	Felon in Possession of Firearms and Ammunition.

The application is based on these facts:
See Attachment C, which is attached and fully incorporated herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Buckrop, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/07/2017

Judge's signature

City and state: Las Cruces, New Mexico

Stephan M. Vidmar, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as the storage unit #173 at Discount Storage, located at 2499 El Camino Real, Las Cruces, New Mexico 88007. The SUBJECT PREMISES is described as a 5 ft. x 5 ft. commercial storage unit, located amongst approximately 600 other units. The facility is gated and the individual unit (#173) is padlocked.

ATTACHMENT B

Items to be Seized

1. Any firearms, firearm parts, firearm accessories, or ammunition, and any documents and records related thereto.

2. Documents and records, including any computer and electronic storage media which may contain records, related to the "SUBJECT OFFENSES," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

   a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

   b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

   c. Records related to the email addresses jkgammell@gmail.com, and thepicklator@aol.com;

d. Records related to the email addresses ending in @yahoo.com or 15@gmail.com that also contain the name of former Washburn Computer Group employees.

e. Records related to payments made to DDoS-for-hire services;

f. Records related to the use of Coinbase;

g. Records related to the moniker "anonrooster;"

h. Records related to the moniker "AnonCunnilingus;"

i. Records related to the online group "Anonymous;"

j. Records reflecting conduct in violation of 18 U.S.C. § 1030;

k. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

8. evidence of the times the COMPUTER was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

11. records of or information about Internet Protocol addresses used by the COMPUTER;

12. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies,

"bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

13. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Attachment C

I, Ryan Buckrop, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since August 2016. I am currently assigned to the Albuquerque Division at the Las Cruces Resident Agency in Las Cruces, New Mexico.

2. During the course of this investigation, I have consulted with other FBI Agents and other law enforcement officers who have extensive experience investigating computer-related offenses and who have assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search storage unit #173 at the Discount Storage facility located at 2499 El Camino Real, Las Cruces, New Mexico 88007 ("SUBJECT LOCATION"), which is more fully described in Attachment A, attached hereto and incorporated herein.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable

to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates, 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." During the course of this investigation, I learned that the target of the investigation, John Kelsey Gammell, was prohibited from possessing firearms or ammunition and that he has nevertheless possessed a handgun, parts for assault rifles, and ammunition, in violation of 18 U.S.C. § 922(g).

6. Located within the premises and item to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 922(g) and 1030(a)(5)(A) (the "SUBJECT OFFENSES").

7. I have worked in close coordination with FBI Minneapolis Special Agent Brian W. Behm, who is the case agent for the Minneapolis-based investigation, and whose statements I believe to be truthful.

8. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that

evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 922(g) and 1030(a)(5)(A), are presently located at the SUBECT LOCATION.

9. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Subject Premises

10. The SUBJECT LOCATION is specifically described as storage unit #173 at the Discount Storage facility, located at 2499 El Camino Real Las Cruces, New Mexico 88007.

Background

11. On May 30, 2017, the Honorable Gregory J. Fouratt signed a warrant authorizing the search of a residence belonging to the father of John Kelsey Gammell, located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, where Gammell had been living recently until traveling to Denver, Colorado for temporary employment. The warrant was based on an Affidavit prepared by your Affiant, which is attached hereto as Exhibit 1, and incorporated by reference.

12. On May 31, 2017, your Affiant and other law enforcement executed the search warrant at 4975 Mother Lode Trail, Las Cruces. During the search of the room in which Gammell had been living, FBI agents located, among other things, a gun case containing an owner's manual for a Heckler & Koch P2000 handgun. The gun was missing

from the case. Gammell's father was interviewed by an FBI agent and he stated that he had purchased the P2000 handgun for Gammell "before he left." Gammell is prohibited from possessing firearms or ammunition based on his prior felony convictions, including his 1992 federal conviction for being a felon in possession of a firearm in violation of 18 U.S.C. §§ 922(g)(1) and 924(e)(1) (Crim. File No. 92-127 (HHM) (D. Minn.)). Gammell was released from prison on the felon in possession conviction in 2006, and he finished his period of supervision in 2010. It is illegal for Gammell to possess any firearm. We have not yet located the P2000 handgun.

13. On May 31, 2017, FBI agents executed a search warrant at a hotel room in the Affordable Inns – Denver West, located in a suburb of Denver, Colorado, where Gammell had been staying while he worked a temporary job at computer company in Golden, Colorado. Gammell was arrested at the time of the execution of the warrant. Gammell was the sole occupant of the hotel room at the Affordable Inns. During the search of the hotel room, FBI agents located, among other things, parts for use in the building of AR-15 assault rifles, including an upper receiver, two lower receivers, a pistol grip, a trigger guard, and 15 high-capacity magazines. As noted above, Gammell is prohibited from possessing firearms, which includes possession of the AR-15 receivers because 18 U.S.C. § 921(a)(3) defines "firearm" to include "(A) any weapon . . . which will or is designed to or may readily be converted to expel a projectile by the action of an explosive" and "(B) the frame or receiver of any such weapon."

14. On June 2, 2017, FBI SA Scott Schons spoke with Tyler Toth, the president of Tracer Inc., in Golden, Colorado, where Gammell had been working as a temporary

contract employee. Mr. Toth told SA Schons that he hired Gammell on March 13, 2017. Gammell returned to New Mexico for a period of time in early April, and then returned to work on April 17, 2017. Mr. Toth indicated that Gammell's father had contacted him and told him that Gammell had been arrested. SA Schons asked whether Gammell had a locker or other storage areas at Tracer Inc. and Mr. Toth told SA Schons that Gammell had a desk with drawers as well as a locker. Mr. Toth walked with SA Schons to the desk Gammell had used. SA Schons was aware that we had not located the P2000 handgun and was concerned it might be in the desk, and so he asked Mr. Toth to look in the drawers. Mr. Toth retrieved a box from one of the drawers. When he picked it up, he remarked, "Oh, I know what this is. It is ammunition."

15. The box was a vacuum-sealed brown box with labeling "Nitro Express Shipping Super-Fast, Low Cost," and partial shipping label with address "Shipping Departm[portion torn off] (573) 445-6363, Midway USA, 5875 W. VAN HORN TAVERN RD" and the words "Cartridges Small Arms." SA Schons concluded that it appeared to be a box of ammunition from its appearance. Midway USA is a company located at 5875 West Van Horn Tavern Road, in Columbia, Missouri, that sells and ships ammunition and firearms components. On June 5, 2017, a search warrant was executed on the box and SA Schons found 420 rounds of 5.56 x 45mm full metal jacket rifle ammunition. As noted above, it is illegal for Gammell to possess any ammunition.

16. A search warrant was also executed on June 6, 2017 on a locker used by Gammell at Tracer Inc. During the search of the locker, FBI agents found two receipts for

firearms components, one dated May 21, 2017 from Bravo Company USA Inc., and another dated May 23, 2017 from FedTactical Direct.

17. On May 31, 2017, Gammell's vehicle was searched pursuant to a search warrant in Colorado. A review of the GPS unit in Gammell's car indicated the most recent New Mexico address listed in the GPS unit was the Discount Storage facility on 2499 El Camino Real. On June 5, 2017, I spoke with an employee of the Discount Storage, who advised me that John Gammell rented a 5 ft. x 5 ft. storage unit at the facility (#173). As contact information for the rental, Gammell had provided an address of "Mother Lode Trl;" a phone number of 612-205-8609; and an email address of jkgammell@gmail.com. As noted in the affidavit attached as Exhibit 1, we have concluded that the phone number and email address belong to Gammell. When Gammell was arrested on May 31, 2017, he had several keys in his hotel room, including a key with the number 173 written on it in ink, which is the same number as the storage unit rented by Gammell.

18. The storage unit was last accessed in April 2017. However, on June 1, 2017, Gammell's father went to Discount Storage and paid rental fees for the unit through the end of September 2017. It should also be noted that Gammell's father made the payment on the storage facility the day after Gammell was arrested and search warrants were executed at Gammell's father's residence and the hotel in Colorado.

Conclusion

19. Based on the facts and background information set forth above, as well as the affidavit attached as Exhibit 1, I respectfully submit there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 922(g) and

1030(a)(5)(A) (the SUBJECT OFFENSES), is located in storage unit #173, at Discount Storage, 2499 El Camino Real, Las Cruces, New Mexico 88007 ("SUBJECT LOCATION"), more specifically identified in Attachment A.

20. I, therefore, respectfully request that a search warrant be issued authorizing the search of the storage unit described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein by reference.

Ryan Buckrop
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
this 7th day of June 2017

STEPHAN M. VIDMAR
United States Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Residence and Garage Located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011

Case No. 17MR443

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of New Mexico
(identify the person or describe the property to be searched and give its location):

Residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, more fully described in Attachment A, which is attached and fully incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and fully incorporated herein.

☑ YOU ARE COMMANDED to execute this warrant on or before June 12, 2017 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Gregory J. Fouratt
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 5/30/17 1630

Judge's signature

City and state: Las Cruces, New Mexico

Gregory J. Fouratt, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door is light brown and faces northwest toward Mother Lode Trail. The garage is located on the west side of the house.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related 18 U.S.C. § 1030, the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

c. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

d. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

k. evidence of the times the COMPUTER was used;

l. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

m. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

n. records of or information about Internet Protocol addresses used by the COMPUTER;

o. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

q. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

2017 MAY 30 PM 4:

CLERK-LAS CRUCES

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Residence and Garage Located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011

Case No. 17MR443

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, more fully described in Attachment A, which is attached and fully incorporated herein.

located in the _____ District of New Mexico , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and fully incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1030(a)(5)(A)	Intentional Damage to a Protected Computer

The application is based on these facts:
See Attachment C, which is attached and fully incorporated herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Buckrop, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/30/2017

Judge's signature

City and state: Las Cruces, New Mexico

Gregory J. Fouratt, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door is light brown and faces northwest toward Mother Lode Trail. The garage is located on the west side of the house.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related 18 U.S.C. § 1030, the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

c. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

d. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

k. evidence of the times the COMPUTER was used;

l. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

m. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

n. records of or information about Internet Protocol addresses used by the COMPUTER;

o. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

q. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Attachment C

I, Ryan Buckrop, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since August 2016. I am currently assigned to the Albuquerque Division at the Las Cruces Resident Agency in Las Cruces, New Mexico.

2. During the course of this investigation I have consulted with other FBI agents and other law enforcement officers who have extensive experience investigating computer-related offenses and who have assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search the residence located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 ("Subject Premises"), which is more fully described in Attachment A, attached hereto and incorporated herein.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly

cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."

6. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 1030(a)(5)(A), which relate to the execution of a DDoS attack (the "Subject Offense").

7. I have worked in close coordination with FBI Minneapolis Special Agent Brian W. Behm, who is the case agent for the Minneapolis-based investigation, and whose statements I believe to be truthful.

8. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, are presently located at the SUBECT PREMISES.

9. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Subject Premises

10. The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door

is light brown and faces northwest toward Mother Lode Trail. The attached garage is located on the west side of the house.

11. On March 8, 2016, a Minneapolis FBI agent queried the National Crime Information Center (NCIC) database and found that John Gammell was assigned New Mexico driver's license 514016801 on April 27, 2015, and resided at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011.

12. The city of Las Cruces is located in Dona Ana County in New Mexico. Per a check of the Dona Ana County Assessor's website, the property at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 is owned by Gerald and LaDonna Gammell, whom, based on the investigation, I believe to be Gammell's parents.

13. FBI agents in New Mexico conducted surveillance at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 on February 22, 2017. On the same date, local law enforcement spoke with Gammell at the residence and confirmed he was currently residing at the 4975 Mother Lode Trail address.

14. Gammell was last observed in the Las Cruces, New Mexico area on approximately April 11, 2017. Gammell was subsequently located in the Denver, Colorado area, and is currently staying at an extended stay hotel on the west side of Denver. Gammell is now working at an electronics manufacturing company near his hotel. In the past, Gammell has worked on a contract basis, and has temporarily relocated from the Las Cruces, New Mexico area before eventually returning to the Mother Lode Trail address, and during the time that he was away from the Mother Lode Trail address he left belongings behind, including computer equipment. In late August or early September 2016, Gammell traveled from New Mexico to Vermont for contract employment, where he stayed until approximately the end of October 2016. A review of search warrant results for Gammell's email account jkgammell@gmail.com found that while Gammell was working in Vermont, Gammell's father wrote an email to Gammell on September 14, 2016 asking him what should be done with the computer left behind at Gammell's parents' residence.

Gammell's father describes the computer as "clearly a valuable possession" belonging to Gammell. Gammell's father states he would like to coordinate with Gammell in the future on potentially placing the computer in storage, adding that he is "not running a computer storage unit here." After he was done working in Vermont, Gammell returned to the Mother Lode Trail address at the end of October 2016, and, based on the investigation, it appears he has been living at the Mother Lode Trail address until traveling to Denver in April for employment, which appears to be temporary given that Gammell is renting his hotel room on a week-to-week basis. In light of the fact that Gammell has been staying at the Mother Lode Trail address for the last approximately six months, that he appears to be only temporarily living in Denver, and that he has left belongings, including computer equipment, behind at the Motherlode Trail address when he has had other temporary employment out of New Mexico, I believe it is likely Gammell again left belongings, including computer equipment, at the 4975 Mother Lode Trail address while he is working in Denver and staying at an extended stay hotel. I believe Gammell's computer equipment will contain evidence of Gammell's DDoS activity, further detailed below.

Background

15. The Internet is a worldwide network of computers, computer systems, and other devices. Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

16. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information

is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

17. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

Probable Cause to Believe Crimes Have Been Committed

17. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting its website, www.washburngrp.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shut-down of its website. The attacks have continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

18. FBI agents have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

19. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee

of Washburn. The email addresses both contained the name "LXXXX SXXXXXXXXXX,"[1] an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago. The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

20. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

21. Grand jury subpoenas for subscriber information were subsequently served on Google, for the account lXXXXsXXXXXXXXXX15@gmail.com, and Yahoo, for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. A grand jury subpoena issued to AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Response to a grand jury subpoena issued to Centurylink indicated this IP address was assigned to Gammell's residence (4975 Mother Lode Trail, Las Cruces, New Mexico 88011) at the time the account

[1] Where email addresses or other personally identifiable information of non-targets of this investigation are referenced herein, your affiant has redacted portions of the identifying information to protect the identity of those third parties using "XXX..." In each instance, your affiant knows the full, unredacted identifier.

was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

22. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

23. The investigation discovered that Gammell maintains numerous social media accounts, including Facebook, Twitter, LinkedIn, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed via a grand jury subpoena issued to Google.

Search Warrant Results – jkgammell@gmail.com

24. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. An FBI agent reviewed the records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

25. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

26. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several

individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled "vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

27. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, an FBI agent located payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

28. The website cstress.net is not currently active, however an FBI agent reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

29. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of

$28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two October 20, 2015 emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

30. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

31. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

32. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

33. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

34. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

35. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be

executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

36. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

37. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he

has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

vDOS Records

38. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016. An FBI agent verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the

payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, an FBI agent was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS records with receipts for those payments that located in Gammell's Gmail account obtained via search warrant.

39. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's email address, jkgammell@gmail.com.

40. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

41. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

42. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

43. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Grand jury subpoena results from Centurylink show IP address 75.161.68.161 was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from IXXXXsXXXXXXXXXX15@gmail.com. As mentioned above, email account IXXXXsXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

44. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. An FBI agent was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

1. Wells Fargo (two IP addresses);

2. JP Morgan Chase Bank;

3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

45. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his

message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

Computers and Telephones

46. Your affiant requests permission to search for and seize the records, documents, and/or materials described in the Attachment B ("Items To Be Seized"). These records, documents, and materials may constitute evidence and/or instrumentalities of crime. These items may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

47. These records, documents, and/or materials may be in the form of paper or stored in the form of computer hardware, software, and electronic files. Businesses and individuals use computers and cell phones at their business and residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.

48. This affidavit also requests permission to seize computer hardware and cell phones that may contain records and documents if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In fact, both Google (which operates Gmail) and Twitter offer dedicated apps for their customers' cell phones.

49. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

50. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

51. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive (or similar media) to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

52. Based on the facts and background information set forth above, I respectfully submit there is probable cause to believe that evidence of a criminal offense, namely, violation of 18 U.S.C. § 1030, is located within the SUBJECT PREMISES, a residence located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, which is more fully described in Attachment A, attached hereto and incorporated herein.

53. I, therefore, respectfully request that a search warrant be issued authorizing the search of the residence described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein for reference.

Ryan Buckrop
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
this 30TH day of May 2017

Gregory J. Tourait
United States Magistrate Judge

EXHIBIT E

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Residence and Garage Located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011

Case No. 17MR443

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of New Mexico
(identify the person or describe the property to be searched and give its location):

Residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, more fully described in Attachment A, which is attached and fully incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and fully incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before June 12, 2017 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Gregory J. Fouratt
(United States Magistrate Judge).

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 5/30/17 1638

Judge's signature

City and state: Las Cruces, New Mexico

Gregory J. Fouratt, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door is light brown and faces northwest toward Mother Lode Trail. The garage is located on the west side of the house.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related 18 U.S.C. § 1030, the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

c. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

d. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

k. evidence of the times the COMPUTER was used;

l. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

m. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

n. records of or information about Internet Protocol addresses used by the COMPUTER;

o. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

q. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Residence and Garage Located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011

Case No. 17MR443

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, more fully described in Attachment A, which is attached and fully incorporated herein.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, which is attached and fully incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1030(a)(5)(A)	Intentional Damage to a Protected Computer

The application is based on these facts:
See Attachment C, which is attached and fully incorporated herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Buckrop, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/30/2017

Judge's signature

City and state: Las Cruces, New Mexico

Gregory J. Fouratt, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door is light brown and faces northwest toward Mother Lode Trail. The garage is located on the west side of the house.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related 18 U.S.C. § 1030, the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

c. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

d. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

k. evidence of the times the COMPUTER was used;

l. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

m. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

n. records of or information about Internet Protocol addresses used by the COMPUTER;

o. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

q. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Attachment C

I, Ryan Buckrop, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since August 2016. I am currently assigned to the Albuquerque Division at the Las Cruces Resident Agency in Las Cruces, New Mexico.

2. During the course of this investigation I have consulted with other FBI agents and other law enforcement officers who have extensive experience investigating computer-related offenses and who have assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search the residence located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 ("Subject Premises"), which is more fully described in Attachment A, attached hereto and incorporated herein.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly

cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."

6. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 1030(a)(5)(A), which relate to the execution of a DDoS attack (the "Subject Offense").

7. I have worked in close coordination with FBI Minneapolis Special Agent Brian W. Behm, who is the case agent for the Minneapolis-based investigation, and whose statements I believe to be truthful.

8. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, are presently located at the SUBECT PREMISES.

9. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Subject Premises

10. The SUBJECT PREMISES is specifically described as the residence and garage located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011. The SUBJECT PREMISES is described as a one story single-family home built in the adobe style. The home is painted white. The wooden front door

is light brown and faces northwest toward Mother Lode Trail. The attached garage is located on the west side of the house.

11. On March 8, 2016, a Minneapolis FBI agent queried the National Crime Information Center (NCIC) database and found that John Gammell was assigned New Mexico driver's license 514016801 on April 27, 2015, and resided at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011.

12. The city of Las Cruces is located in Dona Ana County in New Mexico. Per a check of the Dona Ana County Assessor's website, the property at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 is owned by Gerald and LaDonna Gammell, whom, based on the investigation, I believe to be Gammell's parents.

13. FBI agents in New Mexico conducted surveillance at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 on February 22, 2017. On the same date, local law enforcement spoke with Gammell at the residence and confirmed he was currently residing at the 4975 Mother Lode Trail address.

14. Gammell was last observed in the Las Cruces, New Mexico area on approximately April 11, 2017. Gammell was subsequently located in the Denver, Colorado area, and is currently staying at an extended stay hotel on the west side of Denver. Gammell is now working at an electronics manufacturing company near his hotel. In the past, Gammell has worked on a contract basis, and has temporarily relocated from the Las Cruces, New Mexico area before eventually returning to the Mother Lode Trail address, and during the time that he was away from the Mother Lode Trail address he left belongings behind, including computer equipment. In late August or early September 2016, Gammell traveled from New Mexico to Vermont for contract employment, where he stayed until approximately the end of October 2016. A review of search warrant results for Gammell's email account jkgammell@gmail.com found that while Gammell was working in Vermont, Gammell's father wrote an email to Gammell on September 14, 2016 asking him what should be done with the computer left behind at Gammell's parents' residence.

Gammell's father describes the computer as "clearly a valuable possession" belonging to Gammell. Gammell's father states he would like to coordinate with Gammell in the future on potentially placing the computer in storage, adding that he is "not running a computer storage unit here." After he was done working in Vermont, Gammell returned to the Mother Lode Trail address at the end of October 2016, and, based on the investigation, it appears he has been living at the Mother Lode Trail address until traveling to Denver in April for employment, which appears to be temporary given that Gammell is renting his hotel room on a week-to-week basis. In light of the fact that Gammell has been staying at the Mother Lode Trail address for the last approximately six months, that he appears to be only temporarily living in Denver, and that he has left belongings, including computer equipment, behind at the Motherlode Trail address when he has had other temporary employment out of New Mexico, I believe it is likely Gammell again left belongings, including computer equipment, at the 4975 Mother Lode Trail address while he is working in Denver and staying at an extended stay hotel. I believe Gammell's computer equipment will contain evidence of Gammell's DDoS activity, further detailed below.

Background

15. The Internet is a worldwide network of computers, computer systems, and other devices. Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

16. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information

is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

17. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

Probable Cause to Believe Crimes Have Been Committed

17. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting its website, www.washburngrp.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shut-down of its website. The attacks have continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

18. FBI agents have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

19. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee

of Washburn. The email addresses both contained the name "LXXXX SXXXXXXXXXX,"[1] an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago. The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

20. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

21. Grand jury subpoenas for subscriber information were subsequently served on Google, for the account lXXXXsXXXXXXXXXX15@gmail.com, and Yahoo, for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. A grand jury subpoena issued to AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Response to a grand jury subpoena issued to Centurylink indicated this IP address was assigned to Gammell's residence (4975 Mother Lode Trail, Las Cruces, New Mexico 88011) at the time the account

[1] Where email addresses or other personally identifiable information of non-targets of this investigation are referenced herein, your affiant has redacted portions of the identifying information to protect the identity of those third parties using "XXX..." In each instance, your affiant knows the full, unredacted identifier.

was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

22. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

23. The investigation discovered that Gammell maintains numerous social media accounts, including Facebook, Twitter, LinkedIn, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed via a grand jury subpoena issued to Google.

Search Warrant Results – jkgammell@gmail.com

24. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. An FBI agent reviewed the records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

25. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

26. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several

individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled "vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

27. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, an FBI agent located payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

28. The website cstress.net is not currently active, however an FBI agent reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

29. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of

$28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two October 20, 2015 emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

30. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

31. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

32. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

33. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

34. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

35. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be

executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

36. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

37. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he

has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

vDOS Records

38. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016. An FBI agent verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the

payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, an FBI agent was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS records with receipts for those payments that located in Gammell's Gmail account obtained via search warrant.

39. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's email address, jkgammell@gmail.com.

40. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

41. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

42. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

43. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Grand jury subpoena results from Centurylink show IP address 75.161.68.161 was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from lXXXXsXXXXXXXXXX15@gmail.com. As mentioned above, email account lXXXXsXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

44. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. An FBI agent was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

   1. Wells Fargo (two IP addresses);

   2. JP Morgan Chase Bank;

   3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on FBI review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

45. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his

message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

Computers and Telephones

46. Your affiant requests permission to search for and seize the records, documents, and/or materials described in the Attachment B ("Items To Be Seized"). These records, documents, and materials may constitute evidence and/or instrumentalities of crime. These items may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

47. These records, documents, and/or materials may be in the form of paper or stored in the form of computer hardware, software, and electronic files. Businesses and individuals use computers and cell phones at their business and residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.

48. This affidavit also requests permission to seize computer hardware and cell phones that may contain records and documents if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In fact, both Google (which operates Gmail) and Twitter offer dedicated apps for their customers' cell phones.

49. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

50. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

51. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive (or similar media) to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

52. Based on the facts and background information set forth above, I respectfully submit there is probable cause to believe that evidence of a criminal offense, namely, violation of 18 U.S.C. § 1030, is located within the SUBJECT PREMISES, a residence located at 4975 Mother Lode Trail, Las Cruces, New Mexico 88011, which is more fully described in Attachment A, attached hereto and incorporated herein.

53. I, therefore, respectfully request that a search warrant be issued authorizing the search of the residence described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein for reference.

Ryan Buckrop
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
this 30TH day of May 2017

Gregory J. Fouratt
United States Magistrate Judge

EXHIBIT F

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 17-sw-5773-CBS
A locker located at Tracer Inc., 13551 W 43rd Drive, Golden, Colorado 80403, Unit P, as well as a package retrieved from Tracer Inc., more fully described in Attachment A, attached hereto.	)	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed *(identify the person or describe the property to be seized):*

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(g)	Unlawful Possession of a Firearm or Ammunition
18 U.S.C. § 1030(a)(5)(A)	Intentional Damage to a Protected Computer

The application is based on these facts:

X Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Brian W. Behm
Applicant's signature

FBI Special Agent Brian W. Behm
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***1:28 pm, Jun 05, 2017***

Judge's signature

City and state: Denver, CO

Craig B. Shaffer
United States Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Location to be Searched

The location to be searched is specifically described as a locker for use by John Gammell, located at Tracer Inc., 13551 W 43rd Drive, Golden, Colorado 80403, Unit P, as well as a package retrieved from Tracer Inc., described as a vacuum-sealed brown box with labeling "Nitro Express Shipping Super-Fast, Low Cost," and partial shipping label with address "Shipping Departm[portion torn off] (573) 445-6363, Midway USA, 5875 W. VAN HORN TAVERN RD" and words "Cartridges Small Arms."

ATTACHMENT B

Items to be Seized

1. Any firearms, firearm parts, firearm accessories, or ammunition, and any documents and records related thereto.

2. Documents and records, including any computer and electronic storage media which may contain records, related to the "SUBJECT OFFENSES," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

   a. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;

   b. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;

   c. Records related to the email addresses jkgammell@gmail.com, and thepicklator@aol.com;

   d. Records related to the email addresses ending in @yahoo.com or 15@gmail.com that also contain the name of former Washburn Computer Group employees.

   e. Records related to payments made to DDoS-for-hire services;

   f. Records related to the use of Coinbase;

   g. Records related to the moniker "anonrooster;"

h. Records related to the moniker "AnonCunnilingus;"

i. Records related to the online group "Anonymous;"

j. Records reflecting conduct in violation of 18 U.S.C. § 1030;

k. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

8. evidence of the times the COMPUTER was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

11. records of or information about Internet Protocol addresses used by the COMPUTER;

12. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

13. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brian W. Behm, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since May 2004. I am currently assigned to the Minneapolis Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, Internet and computer intrusion offenses.

2. This affidavit is submitted in support of an application for a warrant to search a locker located at Tracer Inc., 13551 W 43rd Drive, Golden, Colorado, 80403, Unit P, as well as a package retrieved from Tracer Inc., more specifically identified in Attachment A.

3. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates, 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." During the course of this investigation, I learned that the target of the investigation, John Kelsey Gammell, was prohibited from possessing firearms and that he has nevertheless possessed both a handgun and parts for assault rifles in violation of 18 U.S.C. § 922(g).

4. Located within the premises and item to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 922(g) and 1030(a)(5)(A) (the "SUBJECT OFFENSES").

5. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 922(g) and 1030(a)(5)(A), are presently located at the places described in Attachment A.

6. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

7. On May 26, 2017, the Honorable Kristen L. Mix signed a warrant authorizing the search of a hotel room rented by John Kelsey Gammell, located at Affordable Inns – Denver West, Room 149, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033. The warrant was based on an Affidavit prepared by your Affiant, which is attached hereto as Exhibit 1, and incorporated by reference.

8. On May 31, 2017, your Affiant and other law enforcement executed the search warrant at the Affordable Inns – Denver West, and arrested John Kelsey Gammell. Gammell was the sole occupant of the hotel room. During the search of the hotel room, we located, among other things, parts for use in the building of AR-15 assault rifles, including an upper receiver, two lower receivers, a pistol grip, a trigger guard, and 15 high-capacity magazines. Gammell is prohibited from possessing firearms or ammunition based on his prior felony convictions, including his 1992 federal conviction for being a felon in possession of a firearm in violation of 18 U.S.C. §§ 922(g)(1) and 924(e)(1) (Crim. File No. 92-127 (HHM) (D. Minn.)). Gammell was released from prison on the felon in possession conviction in 2006, and he finished his period of supervision in 2010. Gammell is prohibited from possessing the AR-15 receivers because 18 U.S.C. § 921(a)(3) defines "firearm" to include "(A) any weapon . . . which will or

is designed to or may readily be converted to expel a projectile by the action of an explosive" and "(B) the frame or receiver of any such weapon."

9. A search warrant was also conducted on May 31, 2017 at the residence of Gammell's parents in Las Cruces, New Mexico, where Gammell had been living recently until traveling to Denver, Colorado for temporary employment. During the search of the room in which Gammell was living, FBI agents located, among other things, a gun case containing an owner's manual for a Heckler & Koch P2000 handgun. The gun was missing from the case. Gammell's father was interviewed by an FBI agent and he stated that he had purchased the P2000 handgun for Gammell "before he left." As noted above, it is illegal for Gammell to possess any firearm. We have not yet located the P2000 handgun.

10. I learned that in March, April, and May of 2017, Gammell was working at Tracer Inc., in Golden, Colorado, as a temporary contract employee. On June 2, 2017, FBI SA Scott Schons met with the President of Tracer Inc., Tyler Toth, at Tracer Inc.'s business location located at 13551 W 43rd Drive, Unit O, Golden, Colorado 80403. Mr. Toth told SA Schons that he hired Gammell on March 13, 2017. Gammell returned to New Mexico for a period of time in early April, and then returned to work on April 17, 2017. Mr. Toth indicated that Gammell's father had contacted him and told him that Gammell had been arrested. SA Schons asked whether Gammell had a locker or other storage areas at Tracer Inc. and Mr. Toth told SA Schons that Gammell had a desk with drawers as well as a locker. Mr. Toth walked with SA Schons to the desk Gammell had used. SA Schons was aware that we had not located the P2000 handgun and was concerned it might be in the desk, and so he asked Mr. Toth to look in the drawers. Mr. Toth retrieved a box from one of the drawers. When he picked it up, he remarked, "Oh, I know what this is. It is ammunition."

11. The box was a vacuum-sealed brown box with labeling "Nitro Express Shipping Super-Fast, Low Cost," and partial shipping label with address "Shipping Departm[portion torn off] (573) 445-6363, Midway USA, 5875 W. VAN HORN TAVERN RD" and the words "Cartridges Small Arms." It was vacuum-sealed. SA Schons concluded that it appeared to be a box of ammunition from its appearance.

Midway USA is a company located at 5875 West Van Horn Tavern Road, in Columbia, Missouri, that sells and ships ammunition and firearms components.

12. After consulting with the US Attorney's Office, SA Schons asked Mr. Toth if he could take possession of the box for safekeeping, and Mr. Toth agreed to turn the box over to him. We have not yet opened the box. Rather, we decided to apply for a warrant to do so.

13. Mr. Toth also indicated that Gammell was assigned a locker at Tracer Inc. We have not yet searched the locker, and instead are seeking a warrant to authorize such a search.

Conclusion

14. Based on the facts and background information set forth above, as well as the affidavit attached as Exhibit 1, I respectfully submit there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 922(g) and 1030(a)(5)(A) (the SUBJECT OFFENSES) is located in a locker at Tracer Inc., 13551 W 43rd Drive, Unit P, Golden, Colorado 80403, as well as a package retrieved from Tracer Inc., more fully described in Attachment A, attached hereto and incorporated herein.

15. I, therefore, respectfully request that a search warrant be issued authorizing the search of the business location and package described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein by reference.

s/ Brian W. Behm
Brian W. Behm
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me this 5th day of June 2017

United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Julia Martinez, Assistant United States Attorney.

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Affordable Inns – Denver West, Room 149, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033, more fully described in Attachment A, attached hereto.	Case No. 17-sw-5751-KLM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed *(identify the person or describe the property to be seized):*

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Fraud and related activity in connection with computers

The application is based on these facts:

X Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Brian W. Behm
Applicant's signature

[Insert Agents name, Title and Agency name]
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***26 May 2017***

Judge's signature

City and state: Denver, CO

Kristen L. Mix
United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brian W. Behm, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and have been so employed since May 2004. I am currently assigned to the Minneapolis Field Division, Cyber Crimes Squad, which is responsible for the investigation of, among other things, Internet and computer intrusion offenses.

2. During my career as a Special Agent of the FBI, I have participated in numerous investigations involving computer-related offenses, and assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information. In addition to graduating from the FBI Academy in Quantico, Virginia, I have received both formal and informal training in computer-related investigations from the FBI and other organizations.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. This affidavit is submitted in support of an application for a warrant to search the place named in Attachment A.

5. This application and affidavit relate to an ongoing investigation into distributed denial of service ("DDoS") attacks targeting the website of a Minnesota-based company. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack by directing large amounts of internet traffic to the website intended to overwhelm the site. A DDoS attack violates, 18 U.S.C. § 1030(a)(5)(A), Intentional Damage to a Protected Computer, which makes it a crime to "knowingly

cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."

6. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 1030(a)(5)(A), which relate to the execution of a DDoS attack (the "Subject Offense").

7. The statements contained in this affidavit are based in part on information I have learned through the investigation, as well as my experience as an FBI Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, are presently located at the place described in Attachment A.

8. The information contained herein is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

Background

9. The Internet is a worldwide network of computers, computer systems, and other devices. Most users reach the Internet through an Internet Service Provider ("ISP"). The ISP assigns each user an Internet Protocol Address ("IP address"), a set of four numbers, each between 0-255, separated by dots, such as 165.254.24.167. IP addresses are traceable back to the pertinent ISP through publicly available databases.

10. A "domain name" is a logical, text-based equivalent of the numeric IP address; for example, the domain name "uscourts.gov" is assigned the IP address 23.219.160.66. A domain name is generally

associated with a particular IP address and an Internet-connected device. An individual seeking to use a particular domain name can register it with a "domain name registrar," and that registration information is maintained in a publicly-accessible database. An online query – frequently called a "Whois" query – can be used to obtain registration information pertaining to a particular IP address or domain name.

11. Because every device that connects to the Internet must be assigned an IP address, IP address information can help to identify which computers or other devices are communicating over the Internet. This, in turn, can assist in identifying specific Internet users. Conversely, individuals who want to obfuscate their online activity can take a variety of measures to hide this information.

PROBABLE CAUSE

12. Starting on July 30, 2015, the Washburn Computer Group, a company based in Monticello, Minnesota, began experiencing distributed denial of service (DDoS) attacks targeting its website, www.washburngrp.com. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Beginning on or about July 30, 2015, Washburn was subjected to periodic DDoS attacks for more than a year, which resulted in the temporary shut-down of its website. The attacks have continued through at least September 2016, with the attacks also targeting Washburn's newly launched website, www.washburnpos.com, on August 12, 2016.

13. I have reviewed several samples of log files from Washburn's servers showing Internet traffic during the attacks but cannot determine attack attribution from such review. The IP addresses used in connection with the DDoS attack come back to a US-based Virtual Private Network (VPN) that is used to anonymize the true source of incoming Internet access (like many "anonymizing" services, the VPN does not maintain logging information which would show who is using the service).

14. At two different times during which the website DDoS attacks were underway, Washburn management received emails from two different email addresses purporting to be from a former employee of Washburn. The email addresses both contained the name, of an individual who was employed with Washburn for approximately 17 years prior to his termination approximately three and a half years ago: "LXXXX SXXXXXXXXXX."[1] The emails appear to taunt Washburn management regarding ongoing IT issues the company was experiencing - at that time, Washburn's only "ongoing IT issues" were based on the DDoS attacks.

15. The first email, sent on August 11, 2015 from email address lXXXX_sXXXXXXXXXX@yahoo.com, asked how everything was at Washburn and had an attached animation (.gif) of a mouse laughing. The second email, sent October 6, 2015, from lXXXXsXXXXXXXXXX15@gmail.com, again asked how everything was going at Washburn and further inquired if any IT help was needed. Also attached to this second email was an image of a mouse laughing.

16. Subscriber information was obtained from Google on the account lXXXXsXXXXXXXXXX15@gmail.com, and from Yahoo for the account lXXXX_sXXXXXXXXXX@yahoo.com. Analysis of the results showed information connecting both accounts to an individual named John Gammell. Both email addresses were created using the cell phone number 612-205-8609. AT&T Wireless confirmed Gammell as the subscriber of 612-205-8609. In addition, IP address 75.161.68.161 was used when creating the lXXXXsXXXXXXXXXX15@gmail.com account on October 6, 2015, the same day the above email was sent. Centurylink's records reflect this IP address was assigned to Gammell's address (4975 Mother Lode Trail, Las Cruces, New Mexico 88011)

[1] Where email addresses or other personally identifiable information of non-targets of this investigation are referenced herein, your affiant has redacted portions of the identifying information to protect the identity of those third parties using "XXX..." In each instance, your affiant knows the full, unredacted identifier.

at the time the account was created. The lXXXX_sXXXXXXXXXX@yahoo.com account was created using a US-based VPN used to anonymize the true source of Internet traffic.

17. Washburn confirmed that Gammell was a Washburn employee until about three years ago. Gammell left the company on good terms, resigning so he could start his own soldering training company. However, in July 2014, Gammell had a financial dispute with Washburn during negotiations for training Gammell was to provide to Washburn personnel.

18. I discovered that Gammell maintains numerous social media accounts, to include Facebook, Twitter, Linkedln, YouTube, and Freelancer. In addition, I determined that Gammell utilizes email account jkgammell@gmail.com, which was confirmed by business records obtained from Google.

Search Warrant Results – jkgammell@gmail.com

19. A search warrant, dated September 14, 2016, was served on Google for records concerning Gammell's email address, jkgammell@gmail.com. I reviewed the records provided by Google and found numerous items indicating Gammell's involvement with DDoS activity.

20. From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services: "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers."

21. Of the seven DDoS-for-hire websites, search warrant results and vDOS records indicate Gammell made payments to cStress, inboot.me, and vDOS. In email communications with several individuals (detailed further below), Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled

"vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies.

22. Gammell made multiple payments to the DDOS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's email account, I located payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

23. The website cstress.net is not currently active, however I have reviewed the main page via archive.org (dated March 21, 2016), which contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots."

24. On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDOS-for-hire service. On October 20, 2015, Gammell received an email from PayPal which provided an email receipt for a payment of $28.99 to 4ukhost (email account dor.rafel@gmx.com). The transaction was for "Account Funding #3," per the transaction description. Two minutes later on October 20, 2015, Gammell received an email from sales@aiobuy.net thanking him for his purchase with inboot. Based on these two October 20, 2015

emails, I believe Gammell paid for an account at inboot.me, which provided Gammell access to the DDoS-for-hire services provided by inboot.me.

25. On July 23, 2015, Gammell sent an email to DDOS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others.

26. On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address.

27. On May 27, 2016, Gammell received an email from noreply@exostress.in confirming he had registered with DDOS-for-hire service exostress.in.

28. On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDOS-for-hire service.

29. In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company.

30. On July 12, 2015, Gammell sent an email to an individual named Derek, who utilized email address thepicklator@aol.com. Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. The DDoS attacks would be executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and

> powerful "stresser" services. CStress has unlimited boots and VDoS limites to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

31. On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

I believe Gammell's reference to "No bacon here" was intended to indicate that Gammell was not a law enforcement agent.

32. On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted he has memberships at vDOS, cStress, and booter.xyz. Gammell also appears to identify himself as a member of the hacktivist group "Anonymous" at the start of the email. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion?

vDOS Records

33. As mentioned above, one of Gammell's preferred DDoS-for-hire services was vDOS. In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. The vDOS attack logs cover the time-period from approximately April 2016 to July 2016. I have verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information I obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. For example, the payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that I obtained via grand jury subpoena indicating that Gammell paid for the vDOS subscription using his PayPal account. In addition, I was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS

records with receipts for those payments that I located in Gammell's Gmail account I obtained via search warrant.

34. Gammell's known email addresses and usernames were searched against the vDOS records in an effort to identify vDOS accounts created and used by Gammell. The search found two accounts linked to Gammell's jkgammell@gmail.com email address.

35. Gammell's first account was made under the username "anonrooster," with its first observed activity occurring on June 14, 2015. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated with this account for the time period collected.

36. Gammell's second account was made under the username "AnonCunnilingus," with its first observed activity occurring on July 28, 2015. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

37. The payment for $199.99 on December 18, 2015 was corroborated via a Coinbase receipt located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company.

38. A search of the vDOS log files showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. Business records from Centurylink show IP address 75.161.68.161

was assigned to Gerald Gammell at address 4975 Mother Lode Trail, Las Cruces, New Mexico from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from lXXXXsXXXXXXXXXX15@gmail.com. As mentioned above, email account lXXXXsXXXXXXXXXX15@gmail.com was also created using IP address 75.161.68.161 on October 6, 2015.

39. vDOS database records indicate that Gammell utilized the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. I was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, to include those belonging to financial institutions, industrial and manufacturing companies, employment contracting companies, and government organizations. Several entities of note targeted by Gammell are summarized below:

a. Financial Companies -

1. Wells Fargo (two IP addresses);

2. JP Morgan Chase Bank;

3. Hong Kong Exchanges and Clearing Limited (two IP addresses).

b. Government Organizations -

1. Hennepin County (Minnesota) website (hennepin.us);

2. Minnesota Judicial Branch website (mncourts.gov);

3. Dakota County Technical College (dctc.edu).

c. Industrial/Manufacturing Companies and Associations -

1. STI Electronics Inc. (stielectronicsinc.com) – STI Electronics is an electronics and manufacturing company based in Madison, Alabama. Based on my review of the

jkgammell@gmail.com search warrant return, Gammell had business discussions with STI Electronics in March and April 2015;

2. Kit Pack Co. (kitpack.com) – Kit Pack Co. is a company based in Las Cruces, New Mexico. Based on my review of the jkgammell@gmail.com search warrant return, Gammell was employed at Kit Pack Co. in August 2015.

d. Employment Contracting -

1. dmDickason (dmdickason.com) – dmDickason is a staffing and placement company based in El Paso, Texas. Based on my review of the jkgammell@gmail.com search warrant return, Gammell obtained a job with Kit Pack Co through dmDickason, and was in contact with dmDickason in an attempt to secure a job interview in July 2016.

40. Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. Gammell again made reference to being a member of "Anonymous" in these communications and he stated that the target he was referencing did not have his permission to use the internet. The subject of his message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

41. On February 3, 2017, FBI agents conducting surveillance of 4975 Mother Lode Trail, Las Cruces, New Mexico 88011 observed a white Buick Century bearing New Mexico license plate NYY328 parked in the driveway. On February 9, 2017, an FBI agent in New Mexico queried New Mexico's Online Motor Vehicle Record System and learned that Gammell is the registered owner of a white 2003 Buick Century, New Mexico license plate NYY328 (the "SUBJECT VEHICLE"). The vehicle was registered on November 30, 2016, listing Gammell's previous address as 4975 Mother Lode Trail, Las Cruces, New Mexico 88011.

42. On May 1, 2017, FBI agents in Colorado observed Gammell's known vehicle, a 2003 white Buick Century bearing New Mexico license plate NYY328, parked in the Affordable Inns – Denver West, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033 parking lot. Shortly after locating the vehicle, agents saw Gammell entering the vehicle and departing the Affordable Inns – Denver West parking lot. Based on my investigation, your affiant knows that Gammell works short-term jobs around the country. Since approximately April 2015, Gamell has lived with his parents in Las Cruces, New Mexico, but periodically travels for work. Based on your affiant's knowledge of Gammell's work history, he appears to be currently in Denver, Colorado for that purpose.

43. On May 1, 2017, an FBI Task Force member in Colorado contacted the Affordable Inns – Denver West staff and requested a rental roll. A review of the rental roll showed Gammell was staying in Room 149.

44. On May 5, 2017, the United States District Court for the District of Minnesota issued a Pen Register and Trap and Trace order for Gammell's email account, jkgammell@gmail.com. A review of the data generated by the order found IP address 76.120.18.178 frequently was used to login to jkgammell@gmail.com on May 9, 2017 and May 10, 2017, with the logins occurring between approximately 9:00pm and 6:30am Mountain Standard Time. Law enforcement requested subscriber information on IP address 76.120.18.178 on May 9, 2017 and May 10, 2017 from Comcast. On May 24,

2017, Comcast reported that on May 9, 2017 and May 10, 2017, IP address 76.120.18.178 was assigned to Affordable Inns, 10300 South I70 Frontage Road, Wheat Ridge, Colorado 80033. Gammell's use of the hotel internet connection shows he has computer equipment in his possession. In my training and experience, people keep their computers both in their residences, and they keep or transport their computers using their cars. Gammell's computer equipment may have been used in furtherance of his DDoS activity described below, and consequently may contain evidence of the DDoS activity.

Computers and Telephones

45. Your affiant requests permission to search for and seize the records, documents, and/or materials described in the Attachment B ("Items To Be Seized"). These records, documents, and materials may constitute evidence and/or instrumentalities of crime. These items may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

46. These records, documents, and/or materials may be in the form of paper or stored in the form of computer hardware, software, and electronic files. Businesses and individuals use computers and cell phones at their business and residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.

47. This affidavit also requests permission to seize computer hardware and cell phones that may contain records and documents if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In fact, both Google (which operates Gmail) and Twitter offer dedicated apps for their customers' cell phones.

48. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for

forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, "imaging" is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls

for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive (or similar media) to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

51. Based on the facts and background information set forth above, I respectfully submit there is probable cause to believe that evidence of a criminal offense, namely, violation of 18 U.S.C. § 1030, is

located within the place described in Attachment A, which is more fully described in Attachment A, attached hereto and incorporated herein.

52. I, therefore, respectfully request that a search warrant be issued authorizing the search of the residence described in Attachment A, and the search and seizure of the items listed in Attachment B, which is incorporated herein by reference.

s/ Brian W. Behm
Brian W. Behm
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me this 26th day of May 2017

United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Judith Smith, Assistant United States Attorney.

ATTACHMENT A

Description of Location to be Searched

The SUBJECT PREMISES is specifically described as hotel room number 149 at the Affordable Inns – Denver West, 10300 Interstate 70 Frontage Road South, Wheat Ridge, Colorado 80033. The hotel is at the intersection of Interstate 70 Frontage Road South and Miller Street, on the east side of Miller Street.

ATTACHMENT B

Items to be Seized

Any and all records, in whatever form, related to the "Subject Offense," as described in the Affidavit in Support of Search Warrant, which is incorporated by reference herein. Such records include:

1. Records related to possible victims of Denial of Service ("DDoS") attacks, such as Washburn Computer Group, Wells Fargo, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited, Hennepin County (Minnesota) (hennepin.us), the Minnesota Judicial Branch (mncourts.gov), Dakota County Technical College (dctc.edu), STI Electronics Inc. (stielectronicsinc.com), Kit Pack Co. (kitpack.com), and dmDickason (dmdickason.com), as well as other DDoS victims as yet unknown;
2. Records related to DDoS-for-hire services, such as "cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and vdos-s.com ("vDOS"), as well as other DDoS-for-hire services as yet unknown;
3. Records related to the email addresses jkgammell@gmail.com, and thepicklator@aol.com;
4. Records related to the email addresses ending in @yahoo.com or 15@gmail.com that also contain the name of former Washburn Computer Group employees.
5. Records related to payments made to DDoS-for-hire services;
6. Records related to the use of Coinbase;
7. Records related to the moniker "anonrooster,"
8. Records related to the moniker "AnonCunnilingus";
9. Records related to the online group "Anonymous";
10. Records reflecting conduct in violation of 18 U.S.C. § 1030;

11. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media